

REMARKS

Claims 1 and 10 have been amended so the content of the second information is introduced, as previously specified in now cancelled claims 2 and 11. This change is made in response to the final comment in the Response to the arguments, as set forth in the first paragraph on page 4 of the Office Action. Claims 1 and 10 also now require the terminal predetermined data to be concatenated with the first information and the second information to clarify the requirement relating to signing (applying) by the private key of the first member. Concatenating data is obviously known, but claims 1 and 10 require a concatenation of (a) predetermined data, (b) said first information and (c) said second information. Concatenating data does not include the first private key KPRD of the first member (see Office Action, page 7, lines 4-5 from the bottom). The first private key is not transmitted. The first public key KPUBD can be transmitted (e.g. in an electronic certificate; see claim 5) which are signed by using the first private key of said given first member (delegate).

New claims 21 and 22 indicate the predetermined data of claims 1 and 10 include a digitized document.

Independent claims 1 and 10, as amended, distinguish over the combination of Brickell, US Patent Publication 2003/0145223 and Sudia, US Patent 5, 825, 880, the references previously applied against these independent claims, as well as claims 2-8, 11-17, 19 and 20.

Brickell fails to disclose delegating signing predetermined data by a given first member (delegate) mandated by a second member (delegator). Indeed, Brickell discloses data transmission between a delegate mandated by a delegator and a relying party 230 according to credential information of the delegate or the delegator. Furthermore, the office action admits Brickell does not teach reading from the delegate's terminal first information and second information, and transmitting said predetermined data from the delegate's terminal to any user terminal.

Sudia (US 5,825,880) is cited in the office action to disclose processing the first information and second information; i.e. delegate's information and delegator's information. In Sudia (column 27, lines 51 to 66), the primary user (delegator) issues to the delegate a delegation certificate which is signed by the primary user and includes

the delegate's identity and a delegate's public signature verification key. Because the delegation certificate is issued and signed by the primary user, the delegation certificate cannot be properly considered to be the first information and second information that are signed by using the private key of the delegate, i.e. the given first member in claims 1 and 10.

The delegate signs a document with his/her personal signature key and transmits this document as an attachment to the delegation certificate that has been signed by the primary user. The document and attached delegation certificate are transmitted to a document recipient that checks the delegate signature and the delegation certificate. Therefore the Sudia delegate only signs predetermined information (document) and does not sign first information (delegate's identity) and second information (delegator's identity). Consequently, the resulting signature in claim 1 is very different from the Sudia signature.

This difference is very important.

The signature in claims 1 and 10 applies not only to the predetermined data, such as a document processed by the given first member (delegate) in the name of at least a second member (delegator), but also to first information on the first member and second information on the second member, and thus contains a multimember cryptographic delegation mark (page 10, line 20 to page 11, line 2).

The multimember cryptographic delegation mark is not disclosed by Sudia because, in Sudia, the delegation certificate is added to the delegate signature. A certificate added in this way is not necessary or useful for verifying the signature, and is present only for information purposes (page 8, lines 1-5). It can be removed entirely, or other information can be added, without modifying the signature.

The first information (at least the delegate's identity) and second information (at least the delegator's identity) formatted and transmitted with the predetermined data (document) and together signed by the delegate's (given first member's) private key into the signature ensures *a posteriori* in said any user terminal a reliable trace of the relationship between the given first member (delegate) and the second member (delegator), i.e. the titleholder who mandated the given first member as delegate. The "any user terminal" can verify both the delegate's identity and the delegator's identity as

the delegate's private key signed by the two identities.

In amended claims 1 and 10, "concatenating in said terminal predetermined data, said first information and said second information into concatenated data" (page 21, line 3, step E15) emphasizes assembly of the first and second information with the predetermined data to be signed together by the delegate's (given first member's) private key.

Therefore, Sudia fails to suggest the requirements of concatenating and signing in claims 1 and 10. Thus, Sudia fails to disclose transmitting from said terminal said concatenated data and said signature (different from the Sudia signature) to any user terminal.

In Brickell, the delegate signs a service request with his private signature key [0033] to send the service request with a digital certificate and an available delegation certificate to the relaying party (step 330) [0034, 0036]. Brickell fails to disclose a delegate terminal for concatenating the service request and the delegate and delegator information into concatenated data, followed by the delegate signing the concatenated data (and not the service request only). Referring to [0034], the request signature depends only on a delegate private key and a certifying authority key and does not depend on delegate or delegator information which is analogous to the first or second information (identity) from which the signature is produced in claim 1.

Thus, amended claims 1 and 10 are patentable over Brickell in view of Sudia.

Consequently, claims 3-8 and 12-17 are patentable over the combination of Brickell and Sudia. In addition, claims 9 and 18 are patentable over Brickell, Sudia and Garay, US Patent 6,839,436. Garay does not cure the foregoing defects in the rejection of claims 1 and 10.

Early issuance of a Notice of Allowance is courteously solicited.

The Examiner is invited to telephone the undersigned, Applicant's attorney of record, to facilitate advancement of the present application.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 07-1337 and please credit any excess fees to such deposit account.

Respectfully submitted,

LOWE HAUPTMAN HAM & BERNER, LLP

/Allan M. Lowe/

Allan M. Lowe
Registration No. 19,641

USPTO Customer No. 22429
1700 Diagonal Road, Suite 300
Alexandria, VA 22314
(703) 684-1111
(703) 518-5499 Facsimile
Date: February 5, 2009
AML/cjf